E-voting and external voting

Braun Binder, Nadja

10. "E-voting" and external voting*

Nadja Braun

1. Introduction

Electronic voting—'e-voting'—is the option of using electronic means to vote in referendums and elections. Different systems exist, such as direct recording electronic (DRE) voting machines that record the vote directly without that vote being transmitted over the Internet or another network: for example, the interface of a DRE machine can be a touch screen, or the voter can fill out the ballot paper and then scan it into the system. Most commonly, e-voting refers to voting over the Internet using a personal computer (PC) with an Internet connection. There are also other means, such as personal digital assistants (PDAs), telephones or mobile phones, that could be used to cast a vote electronically.

It is useful to distinguish between two concepts of e-voting: 'polling place e-voting', and 'remote e-voting'. 'Polling place e-voting' refers to systems where a voter casts his or her vote inside a polling station or similar premises controlled by electoral staff; 'remote e-voting' is used to describe those systems where a voter casts his or her vote at any place outside the polling station. Both could be relevant for the purposes of this Handbook. There are different ways in which electronic means can be used to facilitate external voting. The most challenging would be to allow voters who are abroad to transmit a vote using electronic means, for example, casting a vote at a PC and transmitting it to the electronic ballot box over the Internet. E-voting could also be carried out in the supervised environment of a diplomatic or consular mission. However, in the course of the research for this paper, no instances of the latter solution being considered were found. Only remote e-voting seems to be an option for external voting.

*The views expressed in this chapter are those of the author and do not necessarily reflect those of the Swiss Federal Chancellery.

Section 2 of this chapter looks into examples where the use of remote e-voting is being considered as a channel for external voting. Section 3 analyses the arguments in favour and against remote e-voting for external voters, and section 4 gives an overview of the most important security challenges and possible approaches to solutions. Apart from the use of electronic means to vote in referendums and elections, electronic means can also be used to support single steps of the external voting process. Section 5 provides some examples of how new information and communications technologies, especially the Internet, can assist an elector abroad. Finally, section 6 draws conclusions from the research.

This survey is based on some examples of what is being done in the field of e-voting and external voting, collected by the Swiss Federal Chancellery. The research is by no means comprehensive and does not take into account each and every country that is practising e-voting or thinking of introducing it. Nor does the chapter look into the discussion about pros and cons of e-voting in general. The list of references and further reading in annex C gives some indications as to where further information about e-voting in general and the discussion about pros and cons can be obtained.

There are very few overviews of e-voting projects worldwide. An overview dating from the summer of 2004 is available on the website of the ACE project at <http://aceproject.org/ace-en/focus/e-voting/>; see also Buchsbaum 2005.

2. Remote e-voting and external voting

Some countries are testing and considering the introduction of remote e-voting especially, and sometimes even exclusively, for their citizens who are living or staying abroad. However, only a few countries allow external voters to cast their votes electronically. Furthermore, there are a few experiments with remote e-voting for external electors, and sometimes expressions of political intentions to consider the question of remote e-voting for external electors. This section highlights some examples of countries that are considering remote e-voting for their citizens abroad.

Austria

In Austria, e-voting is not a top priority for the government. Nevertheless, the Austrian Federal Council of Ministers approved an e-government strategy in May 2003, in which e-voting is listed as a project in the annex, and in the spring of 2004 the Federal Ministry of Interior established a working group on e-voting in order to study and report on various aspects of e-voting (Federal Chancellery 2003; and <http://www.bmaa.gv.at/view.php3?f_id=6016&LNG=de&version>). The working group was not dealing with the question of e-voting for external electors. However, the explanatory memorandum to the Austrian Federal Act on Provisions Facilitating Electronic Communication with Public Bodies (the e-Government Act, available in English at <http://www.ris.bka.gv.at/erv/erv_2004_1_10.pdf>), which came into force on 1 March 2004, explains the provision for setting up a supplementary electronic register as 'a first step towards

enabling Austrian expatriates in future for example to be given the possibility of casting votes at Austrian elections in electronic form' (Explanatory memorandum to the act, in German). In early 2007, the Federal Council of Ministers affirmed its willingness to look into remote e-voting as an additional means of voting as part of a bigger reform of democracy (see <http://www.wienerzeitung.at/DesktopDefault.aspx?TabID=3858&Alias=wzo&cob=274850>).

Estonia

Discussions on remote e-voting started in Estonia in 2001 and one year later, the legal provisions for it were put in place. During summer 2003 the National Electoral Committee started the e-voting project. The system includes the use of smart cards and electronic signatures (see National Election Committee 2005). The first tests of the remote e-voting system were held in late 2004 and 2005 during local referendums and elections. In March 2007 Estonia held the world's first national Internet election. A total of 30,275 citizens (3.4 per cent) used remote e-voting which was available to Estonian voters in Estonia as well as abroad (see National Election Committee, 'E-voting Project').

France

On 1 June 2003, French citizens residing in the USA were given the possibility of electing their representatives to the Council of French Citizens Abroad (Conseil supérieur des Français de l'étranger, CSFE; since 2004 the Assemblée des Français de l'étranger, AFE) by remote e-voting. The AFE is a public law body that is allowed to elect 12 members of the upper house of the French Parliament, the Senate. In 2003, the Forum des droits sur l'internet (Internet Rights Forum), a private body supported by the French Government, published recommendations on the future of e-voting in France. It recommended that remote e-voting should not be introduced, except for French citizens abroad who should be able to elect the CSFE by voting over the Internet (see Internet Rights Forum 2003). For the elections of 18 June 2006 all French citizens abroad were able to choose between three voting channels—personal voting, postal voting or electronic voting (Ministry of Foreign Affairs March 2006).

The Netherlands

In most districts in the Netherlands, voting is done electronically at polling stations. The Dutch Government is also considering and testing remote e-voting (<http://www.minbzk.nl/uk/different_government/remote_e-voting_in>; and Caarls 2004). Dutch nationals resident abroad are entitled to vote in elections to the House of Representatives and the European Parliament (Hupkes 2005). They have to register with the municipality of The Hague for each individual legislative or European election. Dutch electors resident abroad are considered to be an ideal test group for an experiment with e-voting and telephone voting because they are already permitted to vote by post. The purpose of the e-voting project was to ease access for electors abroad and to encourage their participation in elections. The evaluation of the use of e-voting during the elections to the European Parliament in June 2004 showed that e-voting had an added value and made voting

more accessible. Subsequently, in the legislative elections in November 2006, Internet voting was made available again as an experiment and an alternative to postal voting for Dutch voters abroad. A total of 19,815 valid ballots were cast in this way (see <http://www.minbzk.nl/bzk2006uk/subjects/constitution_and/internet_elections>).

Spain

Since 1995, the Generalitat de Catalunya, the government of the autonomous region of Catalonia in north-eastern Spain, has run several pilot projects in parallel with public elections using electronic voting machines inside polling stations. In November 2003, a non-binding remote e-voting pilot was held in parallel with elections to the Catalan Parliament. Over 23,000 Catalans resident in Argentina, Belgium, the United States, Mexico and Chile were invited to participate using any computer connected to the Internet. The Generalitat de Catalunya sponsored this pilot to examine the use of secure electronic voting in the future (see <http://www.gencat.net/governacio-ap/eleccions/e-votacio.htm>).

Switzerland

In August 2000 the Swiss Government gave the Federal Chancellery the task of examining the feasibility of remote e-voting. An interim report of the Swiss Federal Chancellery on remote e-voting called Swiss living or staying abroad 'the most suitable target group' because remote e-voting could save them time, increase effectiveness and save costs (Federal Chancellery August 2004). Since 2002, a variety of legally binding tests of remote e-voting have been carried out in the cantons of Geneva (see <http://www.ge.ch/evoting>), Neuchâtel (see <http://www.guichetunique.ch>) and Zurich (see <http://www.statistik.zh.ch/produkte/evoting/index.php?p=5>), including between 2004 and 2006 seven remote e-voting trials on the occasion of national referendums. The pilot projects were evaluated in 2005 for a number of different aspects, including the potential of remote e-voting to increase voter turnout, the security risks and its cost-effectiveness. The evaluation has shown that remote e-voting is feasible in Switzerland (see Federal Chancellery, <http://www.bk.admin.ch/themen/pore/evoting/00776>). In March 2007 the Swiss Parliament adopted the legal basis for harmonizing the voter registers for Swiss voters abroad. This is the first step towards the offering the Swiss abroad the possibility of remote e-voting, for which there is a strong demand (see <http://www.aso.ch>).

The USA

The USA built an Internet-based electronic voting system for the US Department of Defense's Federal Voting Assistance Program (FVAP). The SERVE voting system, as it was called (Secure Electronic Registration and Voting Experiment), was planned for deployment in the 2004 primary and general elections, and would have allowed the electors overseas and military personnel to vote entirely electronically via the Internet from anywhere in the world. It was expected that up to 100,000 votes would be cast electronically. However, SERVE was stopped in the spring of 2004 following a report by four members of a review group financed by the Department of Defense. They recommended that the development of SERVE be shut down immediately because they considered the Internet and the PC not to be sufficiently secure (Jefferson et al. 2004).

3. Arguments in favour of and against remote e-voting for external electors

3.1. In favour

The common denominator in the seven countries mentioned above is the fact that they wish to make it easier for their citizens abroad to participate in national elections and referendums. In that respect, external electors are considered to be one of the most suitable target groups for remote e-voting, since there is no comparable voting channel fully available for them that would be as comfortable and as accessible. Postal voting—the channel that is probably most comparable to remote e-voting—does not offer the same benefits, since postal services are sometimes too slow for delivering the ballot paper before voting day and thus some external electors are prevented from voting. Other voting channels, such as voting at an embassy or diplomatic mission, are not as convenient for the voter, since he or she needs to go to a certain place during certain hours. The overall thought behind making it easier for external electors to vote in elections and referendums is, of course, to increase voter participation and thus strengthen democratic legitimacy.

Apart from convenience to external electors, there are other reasons in favour of remote e-voting.

1. In some cases, citizens living or staying abroad are considered to be an ideal test group for remote e-voting, while the real intention is to introduce this new method for electors inside the country as well.

2. In some cases, citizens abroad are well organized—even better organized than interest groups inside a country—and capable of formulating their needs and putting them onto the agenda.

3. Depending on the circumstances and the other voting channels available for external electors, remote e-voting might save costs.

3.2. Against

Because by and large only those countries that are considering the introduction of remote e-voting provide information on the subject, there are only a few arguments to be found against the introduction of remote e-voting for external electors. These reasons include:

1. *Security concerns*. However, there are no special security concerns with specific regard to remote e-voting for external electors. Rather, it is remote e-voting as such that is considered to be not secure. The security concerns include doubts about the Internet as a means of transmission of confidential information, fear of hacker attacks—both by insiders (e.g. software programmers) and by outsiders (e.g. political parties, terrorists or other states)—and anxiety about the possibility of undue influence being exerted on the voter during the voting process (e.g. 'family voting').

2. *Financial aspects*. It may be costly to build the infrastructure for providing remote e-voting only to a limited number of electors. The expensive items can be the building of a digitized, harmonized register of external electors or the maintenance of security of the system.

3. *Equal treatment of all electors (external and internal*). In Switzerland for instance, the government says that if remote e-voting is introduced it has to be done on a step-by-step basis. It should be introduced for 'internal' electors first and only after that for external electors. The reason behind this is that there is no centralized electoral register for external electors (see the case study). External electors from one canton should not be able to vote electronically while those from another canton do not have this opportunity.

The Australian Electoral Commission (AEC) answers the question 'Can I vote via the Internet?' on its website (<http://www.aec.gov.au/_content/What/enrolment/faq_os.htm>) as follows:

> The introduction of internet or computerised voting is not a feasible proposition at this time, as a number of security, technical, financial, access and equity issues have to be solved before it could become a fact of electoral life.
> - There is no appropriate software technology for use in full preferential voting system.
> - Many voters, especially the elderly and those with poor literacy and numeracy skills may have difficulty with using the internet.
> - There is a risk of fraud and errors occurring in software without the safeguard of paper ballots to recount.
> - Start up costs would be significant.
> - The AEC would need to continue to provide traditional voting facilities for those with no internet access.

However, Australian electors in Australia have been able to use polling place e-voting for elections to the Australian Capital Territory Legislative Assembly. In 2001 and 2004, e-voting was available at four pre-polling voting centres over a two- to three-week period and at eight polling places on polling day itself (see <http://www.elections.act.gov.au/Elecvote.html>).

4. Some security challenges for remote e-voting and possible solutions

Before remote e-voting is introduced, several security challenges have to be faced. Table 10.1 gives a first idea of the most important of them. However, each country has different legal conditions and different technical infrastructure available. These should be taken into account as well.

Table 10.1: Security challenges for remote voting and possible solutions

Challenges	Possible solutions
Unambiguous identification The participant in a vote or election must be clearly identified and authorized.	• Individual code in order to gain access to the system • Indication of date of birth and the place of origin for the purpose of identity validation and prevention of systematic fraud • Use of a digital signature • Further personal data could be required.
Authenticity of the e-voting servers Citizens must have the guarantee that their votes are sent to the official servers.	• The server certificate should be reviewable by the citizens (fingerprint control). • Authenticity could also be demonstrated by an answer code or symbol (image) which can be verified, e.g. on a polling card sent to the elector by post.
Unique and universal voting Citizens are allowed to cast one vote. The casting of two or more votes must be prevented.	• As soon as an advance vote (postal or electronic) is cast, the voter could be marked in the electronic electoral register. • Unambiguous features on the polling card (e.g. any tampering with the metallic field or seal covering individual ID codes) could indicate that a citizen has probably already cast a vote.
Protection of voting secrecy/protection of privacy The intention of citizens must remain secret and must not be seen by a third party.	• Separate and divided storing of personal data and vote. • Random mixing of votes in the electronic ballot box so that it is impossible to gather knowledge of how someone has voted by comparing the sequence of casting votes and time flags in the electronic electoral register
Hacker attacks to: (a) voting devices (private computers, etc.): possible interception and modification of votes, e.g. by Trojan horses (the weakest point of any e-voting system)	• Firewall protection • Code voting • Virus scans
(b) vote transaction from client to server: possible interception and modification of votes (e.g. man-in-the-middle attack, domain name server (DNS)-hacking).	• Vote encryption • Verification by the voter: vote is transmitted as an image, not as text information • In the transaction dialogue all packages should be check-sum tested (hash code) to prove their integrity
(c) central server platform (heart of the e-voting system), e.g. denial-of-service attack.	• Several redundant servers • Collaboration with major providers

Challenges	Possible solutions
Force majeure Thunderstorms, earthquakes, terrorist attacks etc.	• Several servers at different locations • Housed in highly secure rooms (access control, fire protection, emergency power supply)
Traceability, recounting Electronic votes must be recounted if appealed.	• Voter gets a receipt when his or her vote has been cast • Audit trail journal of the counting of conventional and electronic votes signed by the public servants and controllers in charge • Separate storage (CD-ROM) of electronic votes and log files (encrypted)
Confidence The system and its components must be trustworthy. External experts must be able to review source codes.	• Training of controllers • Use of open-source software (operating system) • Disclosure of proprietary applications

5. Other support through new information and communication technologies

There are also other, less far-reaching ways in which electronic means—among them the Internet—can be used to facilitate voting from abroad. The range goes from providing information to facilitating different steps of the voting process without going so far as to allow voters to cast their ballot electronically. This section highlights some examples.

Australia

Electors abroad can do different things by fax: enrol to vote; apply to become an 'eligible overseas elector'; enrol as spouse or child of an eligible overseas elector; enrol as an 'itinerant elector'; or apply for a postal vote.

New Zealand

Overseas electors can download their ballot paper, declaration and supporting documentation from the Internet starting three weeks before election day. However, they cannot return the ballot papers electronically or vote by email, as the website of Elections New Zealand (<http://www.elections.org.nz/voting/how_vote_overseas.html>) emphasizes. Only overseas electors are allowed to download the ballot paper. Completed ballot papers can be returned by fax or ordinary post. Only voters abroad are allowed to fax their ballot papers; if a ballot paper is faxed from within New Zealand, the vote will not be counted.

Singapore

Singapore offers overseas electors the possibility of filling out a registration form online. However, the form cannot be transmitted over the Internet, but has to be printed out, signed and sent to the Elections Department or any overseas registration centre by registered post. Registered overseas electors are assigned to vote at one of the overseas polling stations (located within Singapore's high commissions, embassies or consulates). If the elector does not remember which his polling station is, he can find out online (<http://www.elections.gov.sg/overseasvoting.htm>).

6. Conclusion

Electors abroad are clearly a focus group that is of particular interest for those countries that are considering the introduction of e-voting in a general manner. At the same time, they are a target group that can be difficult to include in e-voting for practical reasons. Other countries see a need to introduce e-voting for their external electors but do not see the same urgency for introducing e-voting for the internal electors. However, there is no definite trend towards the introduction of remote e-voting, not even in the countries where the first steps towards it have been taken.